ENCLOSURE (F)

AUTHORIZATION FOR OFFICIAL BUSINESS USE

OF COMPUTER RESOURCES

June 1998

U.S. Department of Energy

AUTHORIZATION FOR OFFICIAL BUSINESS USE OF COMPUTING RESOURCES

Type of use:

_____ HEADQUARTERS' COMPUTING RESOURCES OFFSITE, EXCLUDING PORTABLES*
_____ HEADQUARTERS' PORTABLES OFFSITE
_____ HEADQUARTERS' SOFTWARE ON PRIVATELY-OWNED COMPUTERS
_____ PRIVATELY-OWNED COMPUTING RESOURCES OFFSITE
_____ PRIVATELY-OWNED COMPUTING RESOURCES ONSITE*

Description of the intended equipment, software, and/or data to be used; offsite location, configuration, and special service requirements; and the purpose and duration of this use:

I have read, understood, and agree to adhere to the U.S. Department of Energy (DOE) policies for pay administration and hours of work, computer security, data integrity, records management, software copyrights, processing restrictions, liability, and accountability responsibilities outlined in DOE 322.1 and DOE 1360.2B, and other Federal rules and regulations referenced in these Orders and the "Official Sensitive Unclassified Computer and Data Security Policy" stated on the back of this form. (YOU MUST READ THE BACK OF THIS FORM BEFORE SIGNING.)

Employee Signature	Name (Type or Print)	Organization	Date

I DO / DO NOT (circle one) authorize the above employee to use the equipment, software and/or data as described herein. This authorization does not include authorization for overtime compensation or designation of an employee's home as an official duty station.

Program Manager Signature	Name (Type or Print)	Title	Date

* Send a copy of the request to the Office of Administrative Services, either the Forrestal or Germantown Team, for property being taken from or being brought into any DOE Headquarters facility.

Copy to:	❑ Requestor	❑ Organization	❑ Property Management

U.S. Department of Energy

OFFICIAL SENSITIVE UNCLASSIFIED COMPUTER AND DATA SECURITY POLICY

DOE 1360.2B, UNCLASSIFIED COMPUTER SECURITY PROGRAM, establishes the United States (U.S.) Department of Energy (DOE) requirements, policies, responsibilities, and procedures for developing, implementing and sustaining a DOE unclassified computer security program. DOE unclassified computer system shall be protected from abuse and misuse; and sensitive unclassified information shall be protected from unauthorized access, alteration, disclosure, destruction, or improper use as a result of improper actions or adverse events. All information existing in computerized form shall be property safeguarded; and computer processes involved in the collection, creation, manipulation, storage, retrieval, transmission, and display of such information shall be similarity safeguarded both in a manner appropriate to its value to DOE and its potential for loss or disclosure.

All DOE computer hardware, software, and data are U.S. Government property or under license to the U.S. Government, and are to be used for official U.S. Government business only. Therefore, each employee must adhere strictly to the specific security measures and internal controls that have been established for safeguarding the integrity and validity of computer systems and computerized information.

By signing this form, employees indicate they understand the requirements of DOE 1360.2B. The Program Manager (typically a Division Director or Group Leader), at his or her discretion, will then sign the form to authorize the official business use of computer resources requested. Both the employee and Program manager must have an understanding of the requirements of DOE 322.1, PAY AND LEAVE ADMINISTRATION AND HOURS OF DUTY before signing.

Any of the following unauthorized acts in, around, or with computer and telecommunications systems may result in disciplinary action up to and including dismissal in addition to any applicable criminal penalties.

- The introduction of fraudulent records or data into a computer system.
- The unauthorized use of computer facilities.
- The unauthorized alteration or destruction of information or files.
- The theft, whether by electronic means or otherwise, of money, financial instruments, property, services, or valuable data.
- The unauthorized or improper use of logons, passwords, or access codes.
- The reproduction of proprietary software without authorization from the DOE Assistant General Counsel for Intellectual Property.
- Creation and use of classified programs and data without prior approval of the Computer Systems Security Officer (CSSO) within your organization.

Violations or suspected violations of computer security measures or controls should be reported immediately to the Computer Protection Program Manager (CPPM), in the Architecture, Standards, and Engineering Group (HR-43), in the HR Office of Information Management (HR-4).